

Bibliography

DWPI Title

Communication security maintenance method involves authenticating mobile station side apparatus as normal communication party, when data transmitted for authentication and decoded data for authentication are identical

Original Title

COMMUNICATION SECURITY KEEPING METHOD, ITS EXECUTION DEVICE, AND ITS PROCESSING PROGRAM

Assignee/Applicant

Standardized:

HITACHI

LTD

Original: HITACHI LTD

Inventor

ISHIDA SHUICHI ; FUKUZAWA YASUKO ; SETO YOICHI 


Publication Date (Kind Code)

2002-10-11 (A)

Application Number / Date

JP200195052A / 2001-03-29

Priority Number / Date / Country

JP200195052A / 2001-03-29 / JP 

Abstract

Abstract

PROBLEM TO BE SOLVED: To provide a technology that reduces a processing amount performed by using a mobile station key so as to enhance the communication security between a mobile station and a base station.

SOLUTION: The communication security keeping method includes a step of receiving encrypted authentication data from a mobile station that are obtained by encrypting authentication data sent from a base station to a mobile station, a step of decoding the received encrypted authentication data by using the mobile station key of the mobile station, a step of authenticating the mobile station to be a regular communication opposite party when the transmitted authentication data are equivalent to the decoded authentication data, a step of transmitting an authentication consecutive key to continue authentication and a ticket obtained by encrypting the authentication consecutive key with a ticket generating key stored in the base station side unit to the base station authenticated to be a regular communication opposite party, and a step of conducting communication between the base station and the mobile station authenticated to be the regular communication opposite party.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-300152
(P2002-300152A)

(43) 公開日 平成14年10月11日 (2002. 10. 11)

| (51) Int.Cl. ⁷ | 識別記号 | F I | デマコト* (参考) |
|---------------------------|-------|--------------|-------------------|
| H 0 4 L 9/32 | | G 0 9 C 1/00 | 6 4 0 B 5 J 1 0 4 |
| G 0 9 C 1/00 | 6 4 0 | H 0 4 L 9/00 | 6 7 5 A 5 K 0 6 7 |
| H 0 4 Q 7/38 | | H 0 4 B 7/26 | 1 0 9 S |

審査請求 未請求 請求項の数22 O L (全 17 頁)

(21) 出願番号 特願2001-95052(P2001-95052)

(22) 出願日 平成13年3月29日 (2001. 3. 29)

(71) 出願人 000003108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 石田 修一

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 福澤 寧子

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100083552

弁理士 秋田 収喜

最終頁に続く

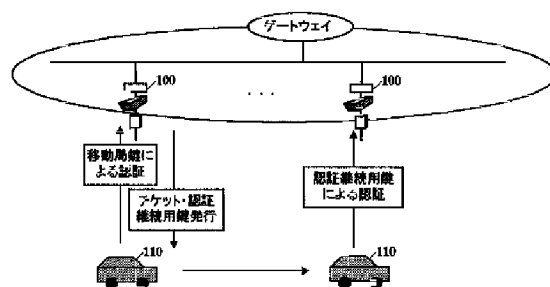
(54) 【発明の名称】 通信セキュリティ保持方法及びその実施装置並びにその処理プログラム

(57) 【要約】

【課題】 移動局鍵を用いた処理量を削減し、移動局と基地局との間の通信セキュリティを高めることが可能な技術を提供する。

【解決手段】 基地局側装置から移動局側装置へ送信された認証用データを暗号化した暗号化認証用データを移動局側装置から受信するステップと、前記受信した暗号化認証用データをその移動局側装置の移動局鍵で復号化するステップと、前記送信した認証用データと前記復号化した認証用データとが等しい場合に当該移動局側装置を正規の通信相手として認証するステップと、正規の通信相手であると認証された移動局側装置に、認証を継続する為の認証継続用鍵と、前記認証継続用鍵を基地局側装置で保持するチケット作成鍵で暗号化したチケットとを送信するステップと、正規の通信相手であると認証された移動局側装置とその基地局側装置との間の通信を行うステップとを有するものである。

図 1



【特許請求の範囲】

【請求項1】 移動局側装置と基地局側装置との間で行われる通信のセキュリティを保持する通信セキュリティ保持方法において、
基地局側装置から移動局側装置へ認証用データを送信するステップと、前記認証用データを暗号化した暗号化認証用データを移動局側装置から受信するステップと、前記受信した暗号化認証用データをその移動局側装置の移動局鍵で復号化するステップと、前記送信した認証用データと前記復号化した認証用データとが等しい場合に当該移動局側装置を正規の通信相手として認証するステップと、
正規の通信相手であると認証された移動局側装置に、認証を継続する為の認証継続用鍵と、前記認証継続用鍵を基地局側装置で保持するチケット作成鍵で暗号化したチケットとを送信するステップと、正規の通信相手であると認証された移動局側装置とその基地局側装置との間の通信を行うステップとを有することを特徴とする基地局側装置の通信セキュリティ保持方法。

【請求項2】 移動局側装置のユーザIDを基地局側装置で保持するマスタ鍵で暗号化して前記移動局鍵を生成するステップを有することを特徴とする請求項1に記載された基地局側装置の通信セキュリティ保持方法。

【請求項3】 移動局側装置から基地局側装置へ送信されたチケットを受信し、そのチケットをチケット作成鍵で復号化して認証継続用鍵を取り出すステップと、基地局側装置から移動局側装置へ認証用データを送信するステップと、前記認証用データを暗号化した暗号化認証用データを移動局側装置から受信するステップと、前記受信した暗号化認証用データを前記取り出した認証継続用鍵で復号化するステップと、前記送信した認証用データと前記復号化した認証用データとが等しい場合に当該移動局側装置を正規の通信相手として認証を継続するステップとを有することを特徴とする請求項1または請求項2のいずれかに記載された基地局側装置の通信セキュリティ保持方法。

【請求項4】 請求項3に記載の処理ステップを複数の基地局側装置で行い、任意の位置の移動局側装置との間の認証継続を実行可能とすることを特徴とする基地局側装置の通信セキュリティ保持方法。

【請求項5】 移動局側装置と基地局側装置との間で行われる通信のセキュリティを保持する通信セキュリティ保持方法において、
基地局側装置から移動局側装置へ送信された認証用データを受信するステップと、前記受信した認証用データをその移動局側装置の移動局鍵で暗号化して暗号化認証用データを生成するステップと、前記生成した暗号化認証用データを基地局側装置へ送信して当該移動局の認証を要求するステップと、
基地局側装置から正規の通信相手として認証された場合

に、認証を継続する為の認証継続用鍵と、前記認証継続用鍵を基地局側装置で保持するチケット作成鍵で暗号化したチケットとを基地局側装置から受信するステップと、その移動局側装置を正規の通信相手として認証した基地局側装置との間の通信を行うステップとを有することを特徴とする移動局側装置の通信セキュリティ保持方法。

【請求項6】 前記移動局鍵は、その移動局側装置のユーザIDを基地局側装置で保持するマスタ鍵で暗号化することにより生成されることを特徴とする請求項5に記載された移動局側装置の通信セキュリティ保持方法。

【請求項7】 前記チケットを基地局側装置へ送信するステップと、基地局側装置から移動局側装置へ送信された認証用データを受信するステップと、前記受信した認証用データを前記認証継続用鍵で暗号化して暗号化認証用データを生成するステップと、前記生成した暗号化認証用データを基地局側装置へ送信して当該移動局の認証継続を要求するステップを有することを特徴とする請求項5または請求項6のいずれかに記載された移動局側装置の通信セキュリティ保持方法。

【請求項8】 基地局側装置やゲートウェイ装置の接続されたネットワーク上での通信のセキュリティを保持する通信セキュリティ保持方法において、
送信データの内容を示すサービスIDに対応した鍵で当該送信データを暗号化して暗号化データを生成するステップと、前記生成した暗号化データをパケットに格納し、そのパケットのヘッダに前記サービスIDを付加してネットワーク上へ送出するステップと、
前記ネットワーク上に送出されたパケットを受信して当該パケットのヘッダに付加されたサービスIDが、その装置で提供されるサービスを示している場合に、当該サービスIDに対応する鍵でそのパケット中の暗号化データを復号化するステップと、前記復号化したデータの内容に従って対応する処理を行うステップとを有することを特徴とする通信セキュリティ保持方法。

【請求項9】 新規にネットワークに接続された基地局側装置を示す接続通知を送信するステップと、前記接続通知が送信された場合に、その基地局側装置を認証する為の認証用データを送信するステップと、新規にネットワークに接続された基地局側装置による認証用データに対する署名を送信するステップと、前記送信された署名を検証し、認証された基地局側装置に対して、前記サービスIDに対応する鍵を示す鍵テーブルを送信するステップを有することを特徴とする請求項8に記載された通信セキュリティ保持方法。

【請求項10】 ネットワークに接続された基地局側装置を監視する為の認証用データを送信するステップと、前記送信された認証用データを基地局側装置で暗号化した暗号化認証用データを送信するステップと、前記送信された暗号化認証用データを検証し、不正に切断された

基地局側装置を検出した場合に、前記サービスIDに対応する鍵を更新するステップを有することを特徴とする請求項8または請求項9のいずれかに記載された通信セキュリティ保持方法。

【請求項11】 移動局側装置との間でセキュリティを保持した通信を行う基地局側装置において、移動局側装置へ送信した認証用データと、移動局側装置から受信した暗号化認証用データをその移動局側装置の移動局鍵で復号化した認証用データとが等しい場合に当該移動局側装置を正規の通信相手として認証する認証処理部と、正規の通信相手であると認証された移動局側装置に、認証を継続する為の認証継続用鍵と、前記認証継続用鍵を基地局側装置で保持するチケット作成鍵で暗号化したチケットとを送信するチケット・鍵発行処理部と、正規の通信相手であると認証された移動局側装置とその基地局側装置との間の通信を行う通信処理部とを備えることを特徴とする基地局側装置。

【請求項12】 移動局側装置のユーザIDを基地局側装置で保持するマスク鍵で暗号化して前記移動局鍵を生成する鍵生成処理部を備えることを特徴とする請求項11に記載された基地局側装置。

【請求項13】 移動局側装置から基地局側装置へ送信されたチケットを受信し、そのチケットをチケット作成鍵で復号化して認証継続用鍵を取り出す鍵取得処理部と、移動局側装置へ送信した認証用データと、移動局側装置から受信した暗号化認証用データをその移動局側装置のチケットから取り出した認証継続用鍵で復号化した認証用データとが等しい場合に当該移動局側装置を正規の通信相手として認証を継続する認証継続処理部とを備えることを特徴とする請求項11または請求項12のいずれかに記載された基地局側装置。

【請求項14】 基地局側装置との間でセキュリティを保持した通信を行う移動局側装置において、基地局側装置から受信した認証用データをその移動局側装置の移動局鍵で暗号化して生成した暗号化認証用データを基地局側装置へ送信して当該移動局の認証を要求する認証要求処理部と、基地局側装置から正規の通信相手として認証された場合に、認証を継続する為の認証継続用鍵と、前記認証継続用鍵を基地局側装置で保持するチケット作成鍵で暗号化したチケットとを基地局側装置から受信するチケット・鍵取得処理部と、その移動局側装置を正規の通信相手として認証した基地局側装置との間の通信を行う通信処理部とを備えることを特徴とする移動局側装置。

【請求項15】 前記移動局鍵は、その移動局側装置のユーザIDを基地局側装置で保持するマスク鍵で暗号化することにより生成されたものであることを特徴とする請求項14に記載された移動局側装置。

【請求項16】 前記チケットと、基地局側装置から受

信した認証用データを前記認証継続用鍵で暗号化して生成した暗号化認証用データを基地局側装置へ送信して当該移動局の認証継続を要求する認証継続要求処理部を備えることを特徴とする請求項14または請求項15のいずれかに記載された移動局側装置。

【請求項17】 基地局側装置やゲートウェイ装置の接続されたネットワーク上での通信のセキュリティを保持する通信セキュリティ保持システムにおいて、送信データの内容を示すサービスIDに対応した鍵で当該送信データを暗号化して暗号化データを生成する暗号化処理部と、前記生成した暗号化データをパケットに格納し、そのパケットのヘッダに前記サービスIDを付加してネットワーク上へ送出するパケット送出処理部と、前記ネットワーク上に送出されたパケットを受信して当該パケットのヘッダに付加されたサービスIDが、その装置で提供されるサービスを示している場合に、当該サービスIDに対応する鍵でそのパケット中の暗号化データを復号化する復号化処理部と、前記復号化したデータの内容に従って対応する処理を行うデータ処理部とを備えることを特徴とする通信セキュリティ保持システム。

【請求項18】 新規にネットワークに接続された基地局側装置を示す接続通知を送信する接続通知処理部と、前記接続通知が送信された場合に、その基地局側装置を認証する為の認証用データを送信する認証用データ送信処理部と、新規にネットワークに接続された基地局側装置による認証用データに対する署名を送信する署名送信処理部と、前記送信された署名を検証し、認証された基地局側装置に対して、前記サービスIDに対応する鍵を示す鍵テーブルを送信する鍵送信処理部とを備えることを特徴とする請求項17に記載された通信セキュリティ保持システム。

【請求項19】 ネットワークに接続された基地局側装置を監視する為の認証用データを送信する監視データ送信処理部と、前記送信された認証用データを基地局側装置で暗号化した暗号化認証用データを送信する生存通知処理部と、前記送信された暗号化認証用データを検証し、不正に切断された基地局側装置を検出した場合に、前記サービスIDに対応する鍵を更新する鍵更新処理部とを備えることを特徴とする請求項17または請求項18のいずれかに記載された通信セキュリティ保持システム。

【請求項20】 移動局側装置との間でセキュリティを保持した通信を行う基地局側装置としてコンピュータを機能させる為のプログラムにおいて、移動局側装置へ送信した認証用データと、移動局側装置から受信した暗号化認証用データをその移動局側装置の移動局鍵で復号化した認証用データとが等しい場合に当該移動局側装置を正規の通信相手として認証する認証処理部と、正規の通信相手であると認証された移動局側装置に、認

証を継続する為の認証継続用鍵と、前記認証継続用鍵を基地局側装置で保持するチケット作成鍵で暗号化したチケットとを送信するチケット・鍵発行処理部と、正規の通信相手であると認証された移動局側装置とその基地局側装置との間の通信を行う通信処理部としてコンピュータを機能させることを特徴とするプログラム。

【請求項21】 基地局側装置との間でセキュリティを保持した通信を行う移動局側装置としてコンピュータを機能させる為のプログラムにおいて、基地局側装置から受信した認証用データをその移動局側装置の移動局鍵で暗号化して生成した暗号化認証用データを基地局側装置へ送信して当該移動局の認証を要求する認証要求処理部と、基地局側装置から正規の通信相手として認証された場合に、認証を継続する為の認証継続用鍵と、前記認証継続用鍵を基地局側装置で保持するチケット作成鍵で暗号化したチケットとを基地局側装置から受信するチケット・鍵取得処理部と、その移動局側装置を正規の通信相手として認証した基地局側装置との間の通信を行う通信処理部としてコンピュータを機能させることを特徴とするプログラム。

【請求項22】 基地局側装置やゲートウェイ装置の接続されたネットワーク上での通信のセキュリティを保持する通信セキュリティ保持システムとしてコンピュータを機能させる為のプログラムにおいて、送信データの内容を示すサービスIDに対応した鍵で当該送信データを暗号化して暗号化データを生成する暗号化処理部と、前記生成した暗号化データをパケットに格納し、そのパケットのヘッダに前記サービスIDを付加してネットワーク上へ送出するパケット送出処理部と、前記ネットワーク上に送出されたパケットを受信して当該パケットのヘッダに付加されたサービスIDが、その装置で提供されるサービスを示している場合に、当該サービスIDに対応する鍵でそのパケット中の暗号化データを復号化する復号化処理部と、前記復号化したデータの内容に従って対応する処理を行うデータ処理部としてコンピュータを機能させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は移動体との通信を行うネットワークでの通信のセキュリティを保持する通信セキュリティ保持システムに関し、特に移動する移動体と移動体の移動エリアをカバーする様に複数設置された基地局との間で行われる通信のセキュリティを保持する通信セキュリティ保持システムに適用して有効な技術に関するものである。

【0002】

【従来の技術】近年、高度道路交通システム(ITS: Intelligent Transport Systems)の構築が行われており、そ

の高度道路交通システムでは、狭域無線通信(DSRC: Dedicated Short Range Communications)を行う車載器を車両に搭載し、車両を停車させることなく自動的に料金の支払いを行う自動料金収受システム(ETC: Electronic Toll Collection system)等の実用化が進められている。

【0003】また前記高度道路交通システムでは、道路に複数の基地局を設置し、移動中の車両に搭載された車載器から最寄りの基地局及びゲートウェイを介してインターネット等のネットワークに接続し、移動中の車両と外部のネットワークとの通信を行うことも検討されている。

【0004】前記の様な高度道路交通システムにおいて、基地局やゲートウェイを接続したネットワークを構成する際には、自律分散システム(ADS: Autonomous Decentralized Systems)が用いられており、この自律分散システムは、相手を特定しない放送型の通信を基礎とし、各ノードが自律的に情報を選択して動作することにより全体が機能するシステムである為、通信の送受信者以外の第三者からの監視、受信者がダウンしたときのバックアップ、システム変更に伴う通信相手の切り替え等を容易に行うことができる。

【0005】

【発明が解決しようとする課題】前記の様に高度道路交通システムにおいて、移動中の車両に搭載された車載器から最寄りの基地局及びゲートウェイを介してインターネット等のネットワークに接続し、有料コンテンツの配信を受ける場合等には、通信時のセキュリティを保持することが重要となる。この場合、車載器と基地局との間で暗号を用いた認証処理を行ってセキュリティを保持することが考えられるが、高速で移動中の車両に搭載された車載器は、短時間で複数の基地局とのハンドオーバーを行う為、車載器と複数の基地局との間の認証処理がハンドオーバーの際に繰り返されると、暗号が解読される可能性が大きくなるという問題がある。

【0006】また前記の様に基地局やゲートウェイとの間の通信で自律分散システムを採用した場合、自律分散システムでは送信先を特定しない放送型の通信が行われる為、送信先の暗号鍵を用いた暗号化が困難であるという問題がある。

【0007】本発明の目的は上記問題を解決し、移動局鍵を用いた処理量を削減し、移動局と基地局との間の通信セキュリティを高めることが可能な技術を提供することにある。本発明の他の目的は、送信先を特定しない放送型の通信を用いた場合でもその通信のセキュリティを高めることが可能な技術を提供することにある。

【0008】

【課題を解決するための手段】本発明は、移動局側装置と基地局側装置との間で行われる通信のセキュリティを保持する通信セキュリティ保持システムにおいて、認証確立時に発行された認証継続用鍵によってそれ以後の認

証継続時の認証を行うものである。

【0009】本発明の通信セキュリティ保持システムにおいて、車両が走行する道路に所定の間隔で基地局側装置を設置しておき、それらの基地局側装置との通信を行う車載器である移動局側装置を搭載した車両がその道路を走行した場合に、まず基地局側装置から移動局側装置へ乱数等の認証用データを送信する。

【0010】基地局側装置から送信された認証用データを受信した移動局側装置では、受信した認証用データを移動局側装置の移動局鍵で暗号化して暗号化認証用データを生成し、その生成した暗号化認証用データを基地局側装置へ送信して当該移動局の認証を基地局側装置へ要求する。

【0011】移動局側装置から送信された暗号化認証用データを受信した基地局側装置では、受信した暗号化認証用データをその移動局側装置の移動局鍵で復号化して認証用データを生成する。ここで、移動局側装置のユーザIDを基地局側装置のマスタ鍵で暗号化して前記移動局鍵を生成するものとしても良い。そして当該移動局側装置へ送信した認証用データと前記復号化した認証用データとを比較して両者が等しい場合に当該移動局側装置を正規の通信相手として認証する。

【0012】その移動局側装置が正規の通信相手として認証されると基地局側装置は、認証を継続する為の認証継続用鍵と、複数の基地局側装置で共有しているチケット作成鍵で前記認証継続用鍵を暗号化して生成したチケットとをその移動局側装置に送信する。移動局側装置では、基地局側装置から送信された前記認証継続用鍵及びチケットを受信した後、その基地局側装置との間の通信を行う。

【0013】本発明の通信セキュリティ保持システムにおいて、移動局側装置を搭載した車両が移動し、他の基地局側装置との通信エリアに入った場合には、その基地局側装置から移動局側装置へ乱数等の認証用データを送信する。

【0014】基地局側装置から送信された認証用データを受信した移動局側装置では、受信した認証用データを前記認証継続用鍵で暗号化して暗号化認証用データを生成し、その生成した暗号化認証用データ及び前記チケットを基地局側装置へ送信して当該移動局の認証継続を基地局側装置へ要求する。

【0015】移動局側装置から送信された暗号化認証用データ及びチケットを受信した基地局側装置では、前記チケットをチケット作成鍵で復号化して認証継続用鍵を取り出した後、前記受信した暗号化認証用データを前記取り出した認証継続用鍵で復号化して認証用データを生成する。そして当該移動局側装置へ送信した認証用データと前記復号化した認証用データとを比較して両者が等しい場合に当該移動局側装置を正規の通信相手として認証を継続する。移動局側装置では、基地局側装置から認

証が継続されたことを示す応答を受信した後、その基地局側装置との間の通信を行う。

【0016】以上の様に本発明の通信セキュリティ保持システムによれば、認証確立時に発行された認証継続用鍵によってそれ以後の認証継続時の認証を行うので、移動局鍵を用いた処理量を削減し、移動局と基地局との間の通信セキュリティを高めることが可能である。

【0017】

【発明の実施の形態】（実施形態1）以下に移動局側装置と基地局側装置との間で行われる通信のセキュリティを保持する実施形態1の通信セキュリティ保持システムについて説明する。

【0018】図1は本実施形態の通信セキュリティ保持システムの概略構成を示す図である。図1に示す様に本実施形態の通信セキュリティ保持システムは、基地局側装置100と、移動局側装置110とを有している。

【0019】基地局側装置100は、車両が走行する道路に所定の間隔で設置された基地局側の装置であり、移動局側装置110との間でセキュリティを保持した通信を行う装置である。移動局側装置110は、複数の基地局が設置された道路を走行する車両に搭載された車載器であり、基地局側装置100との間でセキュリティを保持した通信を行う装置である。

【0020】図1に示す様に本実施形態の通信セキュリティ保持システムでは、基地局側装置100と移動局側装置110との間の最初の認証確立時に基地局側装置100から移動局側装置110へ認証継続用鍵を発行し、他の基地局側装置100と移動局側装置110との間の認証継続時には、前記発行された認証継続用鍵によって認証を行う。

【0021】図2は本実施形態の基地局側装置100の概略構成を示す図である。図2に示す様に本実施形態の基地局側装置100は、CPU201と、RAM202と、ROM203と、入力装置204と、出力装置205と、通信装置206とを有している。

【0022】CPU201は、基地局側装置100全体の動作を制御する装置である。RAM202は、基地局側装置100全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【0023】ROM203は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置204は、移動局側装置110との通信のセキュリティを保持する為の各種入力を行う装置である。出力装置205は、前記セキュリティの保持に伴う各種出力を行う装置である。通信装置206は、ネットワークを介して他の処理装置との通信を行う装置である。

【0024】また基地局側装置100は、認証処理部211と、鍵生成処理部212と、チケット・鍵発行処理部213と、通信処理部214と、認証継続処理部215と、鍵取得処理部216とを有している。

【0025】認証処理部211は、移動局側装置110へ送信した乱数等の認証用データと、移動局側装置110から受信した暗号化認証用データをその移動局鍵で復号化した認証用データとが等しい場合に、その移動局側装置110を正規の通信相手として認証する処理部である。

【0026】鍵生成処理部212は、移動局側装置110のユーザIDを基地局側装置100で保持するマスタ鍵で暗号化して前記移動局鍵を生成する処理部である。チケット・鍵発行処理部213は、正規の通信相手であると認証された移動局側装置110に、認証を継続する為の認証継続用鍵と、前記認証継続用鍵を基地局側装置100で保持するチケット作成鍵で暗号化したチケットとを送信する処理部である。

【0027】通信処理部214は、正規の通信相手であると認証された移動局側装置110とその基地局側装置100との間の通信を行う処理部である。認証継続処理部215は、移動局側装置110へ送信した認証用データと、移動局側装置110から受信した暗号化認証用データをその移動局側装置110のチケットから取り出した認証継続用鍵で復号化した認証用データとが等しい場合に移動局側装置110を正規の通信相手として認証を継続する処理部である。鍵取得処理部216は、移動局側装置110から基地局側装置100へ送信されたチケットを受信し、そのチケットをチケット作成鍵で復号化して認証継続用鍵を取り出す処理部である。

【0028】基地局側装置100を認証処理部211、鍵生成処理部212、チケット・鍵発行処理部213、通信処理部214、認証継続処理部215及び鍵取得処理部216として機能させる為のプログラムは、ROM等の記録媒体に記録されて実行されるものとする。なお前記プログラムを記録する記録媒体はROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0029】図3は本実施形態の移動局側装置110の概略構成を示す図である。図3に示す様に本実施形態の移動局側装置110は、CPU301と、RAM302と、ROM303と、入力装置304と、出力装置305と、通信装置306とを有している。

【0030】CPU301は、移動局側装置110全体の動作を制御する装置である。RAM302は、移動局側装置110全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【0031】ROM303は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置304は、基地局側装置100との通信のセキュリティを保持する為の各種入力を行う装置である。出力装置305は、前記セキュリティの保持に伴う各種出力を行う装置

である。通信装置306は、ネットワークを介して他の処理装置との通信を行う装置である。

【0032】また移動局側装置110は、認証要求処理部311と、チケット・鍵取得処理部312と、通信処理部313と、認証継続要求処理部314とを有している。

【0033】認証要求処理部311は、基地局側装置100から受信した認証用データをその移動局側装置110の移動局鍵で暗号化して生成した暗号化認証用データを基地局側装置100へ送信して当該移動局の認証を要求する処理部である。

【0034】チケット・鍵取得処理部312は、基地局側装置100から正規の通信相手として認証された場合に、認証を継続する為の認証継続用鍵と前記チケットとを基地局側装置100から受信する処理部である。

【0035】通信処理部313は、その移動局側装置110を正規の通信相手として認証した基地局側装置100との間の通信を行う処理部である。認証継続要求処理部314は、前記チケットと、基地局側装置100から受信した認証用データを前記認証継続用鍵で暗号化して生成した暗号化認証用データとを基地局側装置100へ送信して当該移動局の認証継続を要求する処理部である。

【0036】移動局側装置110を認証要求処理部311、チケット・鍵取得処理部312、通信処理部313及び認証継続要求処理部314として機能させる為のプログラムは、ROM等の記録媒体に記録されて実行されるものとする。なお前記プログラムを記録する記録媒体はROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0037】図4は本実施形態の認証確立処理の概要を示す図である。図4に示す様に移動局側装置110は、電源投入後やチケットの有効期限が経過した後に基地局の通信エリアに入ると認証確立処理を開始してその基地局側装置100にユーザIDを送付し、基地局側装置100はマスタ鍵を用いてユーザIDから移動局鍵を生成する。

【0038】なお本実施形態の移動局鍵は、各移動局側装置110のユーザIDをマスタ鍵で暗号化することにより生成され、予め各移動局側装置110へ配布されているものとする。また各基地局側装置100は、各移動局側装置110の移動局鍵自体は保持しておらず、必要に応じてマスタ鍵を用いて各移動局側装置110の移動局鍵を生成して使用するものとする。

【0039】移動局側装置110は、基地局側装置100が発行した認証用データである乱数に対して、移動局側装置110の移動局鍵を用いて暗号化を行う。基地局

側装置100は、移動局側装置110が生成した暗号化認証用データを前記生成した移動局鍵を用いて復号化し、移動局側装置110に送信した認証用データと比較してその移動局の正当性を確認する。

【0040】その移動局の正当性が確認できた場合、基地局側装置100は、認証継続用の鍵と、必要に応じて暗号通信用の鍵、MAC(Message Authentication Code)生成用の鍵を生成して移動局側装置110に発行する。また前記生成した鍵を基地局側装置100のみが共有するチケット作成鍵を用いて暗号化してチケットを生成し、移動局側装置110に送付する。

【0041】図5は本実施形態の認証確立処理のシーケンスを示す図である。図5に示す様に本実施形態では、基地局側装置100から移動局側装置110へ認証用データとして乱数R1を送信し、移動局側装置110から基地局側装置100へは、移動局側装置110のユーザIDと移動局鍵Kaで乱数R1を暗号化したEnc_Ka(R1)を送信する。

【0042】基地局側装置100ではユーザIDから移動局鍵Kaを生成し、送信した乱数R1とEnc_Ka(R1)の復号内容が一致する場合に、基地局ID、ユーザID、有効期限、認証継続用鍵K1、暗号通信用鍵K2、MAC生成鍵K3、正当性チェック用コードをチケット作成鍵Kbで暗号化したチケットCertと、認証継続用鍵K1、暗号通信用鍵K2、MAC生成鍵K3を移動局側装置110に送信する。

【0043】図6は本実施形態の認証継続処理の概要を示す図である。図6に示す様に移動局側装置110は、ある基地局との認証確立後に他の基地局の通信エリアに入ると、認証継続処理を開始してその基地局側装置100にチケットを送付し、基地局側装置100はチケット作成鍵を用いてチケットから認証継続用鍵を取得する。

【0044】また移動局側装置110は、基地局側装置100が発行した認証用データである乱数に対して、移動局側装置110で受信している認証継続用鍵を用いて暗号化を行う。基地局側装置100は、移動局側装置110が生成した暗号化認証用データを前記生成した認証継続用鍵を用いて復号化し、移動局側装置110に送信した認証用データと比較してその移動局の正当性を確認し、その移動局の認証を継続して行う。

【0045】図7は本実施形態の認証継続処理のシーケンスを示す図である。図7に示す様に本実施形態では、基地局側装置100から移動局側装置110へ認証用データとして乱数R2を送信し、移動局側装置110から基地局側装置100へは、チケットCertと認証継続用鍵K1で乱数R2を暗号化したEnc_K1(R2)を送信する。

【0046】基地局側装置100では、チケットCert中の有効期限や正当性チェック用コードによりチケットのチェックを行った後、認証継続用鍵K1を取り出し、前記送信した乱数R2とEnc_K1(R2)の復号内容が一致する場合

に、移動局の認証を継続して行うことを示す認証結果を移動局側装置110に送信する。

【0047】以下に、本実施形態の通信セキュリティ保持システムにおいて、基地局側装置100と移動局側装置110との間の認証確立処理及び認証継続処理の処理手順について説明する。

【0048】図8は本実施形態の基地局側装置100による移動局側装置110の認証確立処理及び認証継続処理の処理手順を示すフローチャートである。図8に示す様にステップ801で基地局側装置100の認証処理部211は、基地局側装置100の通信エリア内に移動局側装置110を検出すると、認証用データとして乱数を移動局側装置110へ送信して認証処理を開始する。

【0049】図9は本実施形態の移動局側装置110から基地局側装置100への認証確立要求処理及び認証継続要求処理の処理手順を示すフローチャートである。図9に示す様にステップ901で移動局側装置110の認証要求処理部311は、認証用データとして乱数を基地局側装置100から受信しているかどうかを調べ、認証用データを受信している場合にはステップ902へ進む。ステップ902では、前記認証用データを送信した基地局側装置100との間の認証処理が未実行であるかどうかを調べ、認証処理が未実行である場合にはステップ903へ進む。ステップ903では、認証を継続する為のチケットを未取得であるかまたは他の基地局側装置100からチケットを受信済みであるかどうかを調べ、チケットを未取得である場合にはステップ904へ進む。ステップ904では、基地局側装置100から受信した認証用データをその移動局側装置110の移動局鍵で暗号化して暗号化認証用データを生成する。ステップ905では、前記生成した暗号化認証用データを基地局側装置100へ送信して当該移動局の認証を要求する。

【0050】ステップ802で基地局側装置100の認証処理部211は、暗号化された認証用データを移動局側装置110から受信しているかどうかを調べ、暗号化認証用データを受信している場合にはステップ811へ進む。

【0051】ステップ811で認証継続処理部215は、前記暗号化認証用データと共にチケットを移動局側装置110から受信しているかどうかを調べ、チケットを受信している場合にはステップ812へ進み、チケットを受信していない場合にはステップ803へ進む。

【0052】ステップ803で認証処理部211は、前記暗号化認証用データと共にユーザIDを移動局側装置110から受信しているかどうかを調べ、ユーザIDを受信している場合にはステップ804へ進む。

【0053】ステップ804で鍵生成処理部212は、移動局側装置110のユーザIDを基地局側装置100のROM203で保持しているマスタ鍵で暗号化してその移動局側装置110の移動局鍵を生成する。ステップ

805で認証処理部211は、前記受信した暗号化認証用データを前記生成した移動局鍵で復号化して認証用データを復元する。

【0054】ステップ806では、その移動局側装置110へ送信した認証用データと、前記復号化した認証用データとを比較し、両者が等しい場合にはステップ807へ進む。ステップ807では、その移動局側装置110を正規の通信相手として基地局側装置100のRAM202に登録する。

【0055】ステップ808でチケット・鍵発行処理部213は、正規の通信相手であると認証された移動局側装置110との間の認証を他の基地局で継続する為の認証継続用鍵を生成し、その認証継続用鍵を前記移動局鍵で暗号化して鍵配布データを生成する。

【0056】ステップ809では、前記生成した認証継続用鍵を基地局側装置100のROM203で保持しているチケット作成鍵で暗号化してチケットを生成する。ここでチケット作成鍵は複数の基地局側装置100で共有された鍵であり、チケットを移動局側装置110で復号化することはできないものとする。

【0057】ステップ810では、その移動局側装置110が認証されたことを示す情報と、前記生成した鍵配布データ及びチケットを移動局側装置110へ送信する。なお前記の処理で暗号通信用鍵やMAC生成鍵を生成し、認証継続用鍵と共に送信しても良い。

【0058】ステップ906で移動局側装置110のチケット・鍵取得処理部312は、前記要求した認証処理の結果として、その移動局側装置110が認証されたことを示す情報と、鍵配送データ及びチケットを基地局側装置100から受信しているかどうかを調べ、認証されたことを示す情報とチケット及び鍵配送データを受信している場合にはステップ907へ進む。

【0059】ステップ907で認証要求処理部311は、その基地局側装置100との間の認証処理を完了したことを示す情報を移動局側装置110のRAM302に登録する。ステップ908では、前記受信した鍵配送データをその移動局側装置110の移動局鍵で復号化して認証継続用鍵を復元してRAM302に格納する。なお前記受信した鍵配送データに暗号通信用鍵やMAC生成鍵が含まれている場合にはそれらの鍵も復元する。ステップ909では、前記受信したチケットを移動局側装置110のRAM302へ格納する。

【0060】一方、ステップ903で認証を継続する為のチケットを未取得であるかどうかを調べた結果、チケットを取得済みである場合にはステップ910へ進む。ステップ910で認証継続要求処理部314は、基地局側装置100から受信した認証用データを前記受信した認証継続用鍵で暗号化して暗号化認証用データを生成する。ステップ911では、前記生成した暗号化認証用データと前記取得済みのチケットを基地局側装置100へ

送信して当該移動局の認証継続を要求する。

【0061】ステップ811で基地局側装置100の認証継続処理部215は、前記暗号化認証用データと共にチケットを移動局側装置110から受信してステップ812へ進む。

【0062】ステップ812で鍵取得処理部216は、移動局側装置110から送信されたチケットをチケット作成鍵で復号化して認証継続用鍵を取り出す。ステップ813で認証継続処理部215は、前記受信した暗号化認証用データを前記取り出した認証継続用鍵で復号化し、認証用データを復元する。

【0063】ステップ814では、その移動局側装置110へ送信した認証用データと、前記復号化した認証用データとを比較し、両者が等しい場合にはステップ815へ進む。ステップ815では、その移動局側装置110を正規の通信相手として基地局側装置100のRAM202に登録する。ステップ816では、前記認証処理の結果として認証の継続が許可されたことを示す情報を移動局側装置110へ送信する。

【0064】ステップ912で移動局側装置110の認証継続要求処理部314は、前記要求した認証処理の結果として、認証の継続が許可されたことを示す情報を基地局側装置100から受信しているかどうかを調べ、認証継続許可を示す情報を受信している場合にはステップ913へ進む。ステップ913では、その基地局側装置100との間の認証処理を完了したことを示す情報を移動局側装置110のRAM302に登録する。

【0065】本実施形態の通信セキュリティ保持システムでは、前記の認証確立処理や認証継続処理が行われた後、基地局側装置100の通信処理部214と移動局側装置110の通信処理部313との間で通信処理を行う。

【0066】以上説明した様に本実施形態の通信セキュリティ保持システムによれば、認証確立時に発行された認証継続用鍵によってそれ以後の認証継続時の認証を行うので、移動局鍵を用いた処理量を削減し、移動局と基地局との間の通信セキュリティを高めることが可能である。

【0067】（実施形態2）以下に基地局側装置やゲートウェイ装置の接続されたネットワーク上での通信のセキュリティを保持する実施形態2の通信セキュリティ保持システムについて説明する。

【0068】図10は本実施形態の通信セキュリティ保持システムの概略構成を示す図である。図10に示す様に本実施形態の通信セキュリティ保持システムは、基地局側装置1000と、ゲートウェイ装置1010と、認証装置1020と、鍵テーブル1030とを有している。

【0069】基地局側装置1000は、車両が走行する道路に所定の間隔で設置された基地局側の装置であり、

移動局からの要求によりゲートウェイ装置1010との間でセキュリティを保持した通信を行う装置である。

【0070】ゲートウェイ装置1010は、基地局側装置1000と外部ネットワークとの間の通信を行う装置であり、基地局側装置1000との間でセキュリティを保持した通信を行う装置である。認証装置1020は、新規にネットワークに接続された基地局側装置1000を認証してサービスIDに対応する鍵を示す鍵テーブル1030の内容を送信し、不正に切断された基地局側装置1000を検出した場合に、前記サービスIDに対応する鍵を更新する装置である。鍵テーブル1030は、送信データの内容を示すサービスIDに対応した鍵を格納するテーブルである。

【0071】図10に示す様に本実施形態の通信セキュリティ保持システムでは、移動局から路側網を経由した上位網のインターネットへの通信等の際に、自律分散プロトコルにより基地局側装置1000とゲートウェイ装置1010との間で送受信される送信データについて、そのサービスIDに対応する鍵を鍵テーブル1030から読み出して暗号化を行う。

【0072】図11は本実施形態の基地局側装置1000の概略構成を示す図である。図11に示す様に本実施形態の基地局側装置1000は、CPU1101と、RAM1102と、ROM1103と、入力装置1104と、出力装置1105と、通信装置1106とを有している。

【0073】CPU1101は、基地局側装置1000全体の動作を制御する装置である。RAM1102は、基地局側装置1000全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【0074】ROM1103は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置1104は、ゲートウェイ装置1010との通信のセキュリティを保持する為の各種入力を行う装置である。出力装置1105は、前記セキュリティの保持に伴う各種出力を行う装置である。通信装置1106は、ネットワークを介して他の処理装置との通信を行う装置である。

【0075】また基地局側装置1000は、暗号化処理部1111と、パケット送出処理部1112と、接続通知処理部1113と、署名送信処理部1114と、生存通知処理部1115とを有している。

【0076】暗号化処理部1111は、送信データの内容を示すサービスIDに対応した鍵で当該送信データを暗号化して暗号化データを生成する処理部である。パケット送出処理部1112は、前記生成した暗号化データをパケットに格納し、そのパケットのヘッダに前記サービスIDを付加してネットワーク上へ送出する処理部である。

【0077】接続通知処理部1113は、新規にネット

ワークに接続された基地局側装置1000を示す接続通知を送信する処理部である。署名送信処理部1114は、認証装置1020から送信された認証用データに対する署名を送信する処理部である。生存通知処理部1115は、認証装置1020から送信された認証用データを暗号化した暗号化認証用データを送信する処理部である。

【0078】基地局側装置1000を暗号化処理部1111、パケット送出処理部1112、接続通知処理部1113、署名送信処理部1114及び生存通知処理部1115として機能させる為のプログラムは、ROM等の記録媒体に記録されて実行されるものとする。なお前記プログラムを記録する記録媒体はROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0079】図12は本実施形態のゲートウェイ装置1010の概略構成を示す図である。図12に示す様に本実施形態のゲートウェイ装置1010は、CPU1201と、メモリ1202と、磁気ディスク装置1203と、入力装置1204と、出力装置1205と、CD-ROM装置1206と、通信装置1207とを有している。

【0080】CPU1201は、ゲートウェイ装置1010全体の動作を制御する装置である。メモリ1202は、ゲートウェイ装置1010全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【0081】磁気ディスク装置1203は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置1204は、基地局側装置1000との通信のセキュリティを保持する為の各種入力を行う装置である。

【0082】出力装置1205は、前記セキュリティの保持に伴う各種出力を行う装置である。CD-ROM装置1206は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。通信装置1207は、インターネットやイントラネット等のネットワークを介して他の処理装置との通信を行う装置である。またゲートウェイ装置1010は、復号化処理部1211と、データ処理部1212とを有している。

【0083】復号化処理部1211は、前記ネットワーク上に送出されたパケットを受信して当該パケットのヘッダに付加されたサービスIDが、その装置で提供されるサービスを示している場合に、当該サービスIDに対応する鍵でそのパケット中の暗号化データを復号化する処理部である。データ処理部1212は、前記復号化したデータの内容に従って対応する処理を行う処理部である。

【0084】ゲートウェイ装置1010を復号化処理部1211及びデータ処理部1212として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0085】図13は本実施形態の認証装置1020の概略構成を示す図である。図13に示す様に本実施形態の認証装置1020は、CPU1301と、メモリ1302と、磁気ディスク装置1303と、入力装置1304と、出力装置1305と、CD-ROM装置1306と、通信装置1307とを有している。

【0086】CPU1301は、認証装置1020全体の動作を制御する装置である。メモリ1302は、認証装置1020全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【0087】磁気ディスク装置1303は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置1304は、新規に接続された基地局側装置1000や不正に切断された基地局側装置1000を管理する為の各種入力を行う装置である。

【0088】出力装置1305は、基地局側装置1000の管理に伴う各種出力を行う装置である。CD-ROM装置1306は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。通信装置1307は、インターネットやイントラネット等のネットワークを介して他の処理装置との通信を行う装置である。

【0089】また認証装置1020は、認証用データ送信処理部1311と、鍵送信処理部1312と、監視データ送信処理部1313と、鍵更新処理部1314とを有している。

【0090】認証用データ送信処理部1311は、ネットワークに接続された基地局側装置1000を認証する為の認証用データを送信する処理部である。鍵送信処理部1312は、前記送信された署名を検証し、認証された基地局側装置1000に対して、前記サービスIDに対応する鍵を示す鍵テーブル1030を送信する処理部である。

【0091】監視データ送信処理部1313は、ネットワークに接続された基地局側装置1000を監視する為の認証用データを送信する処理部である。鍵更新処理部1314は、前記送信された署名を検証し、不正に切断された基地局側装置1000を検出した場合に、前記サービスIDに対応する鍵を更新する処理部である。

【0092】認証装置1020を認証用データ送信処理

部1311、鍵送信処理部1312、監視データ送信処理部1313及び鍵更新処理部1314として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0093】図14は本実施形態の自律分散システムでの暗号通信処理の概要を示す図である。図14に示す様に本実施形態の通信セキュリティ保持システムでは、送信データのサービスIDに対応する鍵で当該送信データを暗号化してネットワーク上へ送出する。ネットワーク上の各装置は、前記送出されたパケットを受信して当該パケットのヘッダに付加されたサービスIDが、その装置で提供されるサービスを示している場合に、当該サービスIDに対応する鍵でそのパケット中の暗号化データを復号化し、そのデータの内容に応じた処理を行う。

【0094】以下に、本実施形態の通信セキュリティ保持システムにおいて、送信データを暗号化し、自律分散プロトコルにより基地局側装置1000からゲートウェイ装置1010へ暗号化データを送信する処理手順について説明する。ここでは、基地局側装置1000からゲートウェイ装置1010への暗号通信について説明するが、暗号化処理部1111及びパケット送出処理部1112をゲートウェイ装置1010に、復号化処理部1211とデータ処理部1212を基地局側装置1000に備え、ゲートウェイ装置1010から基地局側装置1000への暗号通信や、基地局側装置1000同士の暗号通信を行っても良い。

【0095】図15は本実施形態の基地局側装置1000からのデータ送信処理の処理手順を示すフローチャートである。図15に示す様にステップ1501で基地局側装置1000は、移動局から送信データを受信しているかどうかを調べ、送信データを受信している場合にはステップ1502へ進む。ステップ1502で暗号化処理部1111は、送信データの内容を示すサービスIDに対応した鍵をROM1103中の鍵テーブル1030から読み出す。

【0096】図16は本実施形態の鍵テーブル1030の一例を示す図である。図16に示す様に本実施形態の鍵テーブル1030には、サービスIDに対応する暗号鍵が格納されており、データの内容毎に異なる暗号鍵が格納されている。

【0097】ステップ1503で暗号化処理部1111は、前記読み出した鍵で当該送信データを暗号化して暗号化データを生成する。ステップ1504でパケット送出処理部1112は、前記生成した暗号化データをパケ

ットに格納し、そのパケットのヘッダに前記サービスIDを付加してネットワーク上へ送出する。

【0098】図17は本実施形態のゲートウェイ装置1010でのデータ受信処理の処理手順を示すフローチャートである。図17に示す様にステップ1701でゲートウェイ装置1010は、ネットワーク上にパケットが送出されているかどうかを調べ、パケットが送出されている場合にはそのパケットを受信してステップ1702へ進む。

【0099】ステップ1702で復号化処理部1211は、前記受信したパケットのヘッダに付加されているサービスIDを読み出す。ステップ1703では、前記読み出したサービスIDが、その装置で提供されるサービスを示しているかどうかを調べ、その装置で提供されるサービスを示している場合にはステップ1704へ進む。

【0100】ステップ1704では、前記サービスIDに対応する鍵を磁気ディスク装置1203中の鍵テーブル1030から読み出す。ステップ1705では、前記読み出した鍵でそのパケット中の暗号化データを復号化する。ステップ1706でデータ処理部1212は、前記復号化したデータを外部ネットワークへ送出する等、当該データの内容に従って対応する処理を行う。

【0101】前記の様に本実施形態では、送信データの内容を示すサービスIDに対応した鍵で送信データを暗号化してネットワーク上へ送出するので、自律分散システムの様に送信先を特定しない放送型の通信を用いた場合でも、そのデータを暗号化して通信のセキュリティを高めることが可能である。

【0102】前記の様に通信のセキュリティを高める場合には、鍵テーブル1030を適切に管理する必要がある。以下に、本実施形態の通信セキュリティ保持システムにおいて、新規にネットワーク接続された基地局側装置1000が正規の基地局として認証された後に鍵テーブル1030の内容をその基地局側装置1000へ配送する処理について説明する。

【0103】図18は本実施形態の新規基地局の認証処理の概要を示す図である。図18に示す様に本実施形態において、新規にネットワークに接続された基地局側装置1000は認証装置1020に接続通知を送信し、認証装置1020は乱数等の認証用データをその基地局側装置1000へ送信する処理を行う。基地局側装置1000は受信した認証用データに署名を行って認証装置1020に送信し、認証装置1020は、送信された署名を検証した後、鍵テーブル1030をその基地局側装置1000へ送信する処理を行う。

【0104】図19は本実施形態の新規基地局の認証要求処理の処理手順を示すフローチャートである。図19に示す様にステップ1901で基地局側装置1000の接続通知処理部1113は、基地局側装置1000が新

規にネットワークに接続されたことを示す接続通知として、接続通知のサービスIDをヘッダに設定したパケットをネットワーク上に送出する。

【0105】図20は本実施形態の認証装置1020による新規基地局の認証処理の処理手順を示すフローチャートである。図20に示す様にステップ2001で認証装置1020は、ネットワーク上に送出されているパケットのサービスIDを調べ、接続通知が送出されている場合にはその接続通知を受信してステップ2002へ進む。

【0106】ステップ2002で認証用データ送信処理部1311は、ネットワークに接続された基地局側装置1000を認証する為の乱数等の認証用データと、認証用の乱数であることを示すサービスIDとを格納したパケットをネットワーク上に送出する。

【0107】ステップ1902で基地局側装置1000は、ネットワーク上に送出されているパケットのサービスIDを調べ、認証用データが送出されている場合にはその認証用データを受信してステップ1903へ進む。

【0108】ステップ1903で署名送信処理部1114は、前記受信した認証用データに対してその基地局側装置1000の秘密鍵を用いてデジタル署名を行う。ステップ1904では、前記デジタル署名を行った認証用データと、新規接続時の署名であることを示すサービスIDとを格納したパケットをネットワーク上に送出する。

【0109】ステップ2003で認証装置1020は、ネットワーク上に送出されているパケットのサービスIDを調べ、新規接続時の署名が送出されている場合にはその新規接続時の署名を受信してステップ2004へ進む。

【0110】ステップ2004で鍵送信処理部1312は、前記送信された署名をその基地局側装置1000の公開鍵を用いて検証する。なお基地局側装置1000の公開鍵は予め認証装置1020に登録されているものとする。

【0111】ステップ2005では、前記検証結果を参照し、前記送信された署名が正規の基地局側装置1000から送信されていることが検証された場合にはステップ2006へ進む。ステップ2006では、鍵テーブル1030を前記認証された基地局側装置1000の公開鍵で暗号化して鍵配布データを生成し、この鍵配布データと、鍵配布であることを示すサービスIDとを格納したパケットをネットワーク上に送出する。

【0112】ステップ1905で基地局側装置1000は、ネットワーク上に送出されているパケットのサービスIDを調べ、鍵配布データが送出されている場合にはその鍵配布データを受信してステップ1906へ進む。ステップ1906では、前記受信した鍵配布データをその基地局側装置1000の秘密鍵で復号化して鍵テー

ル1030を復元し、ROM1103へ格納する。

【0113】次に、本実施形態の通信セキュリティ保持システムにおいて、不正に切断された基地局側装置1000を検出して鍵テーブル1030の内容を変更する処理について説明する。

【0114】図21は本実施形態の基地局の監視処理の概要を示す図である。図21に示す様に本実施形態において、認証装置1020は、ネットワークに接続された基地局側装置1000を認証する為の乱数等の認証用データを所定の条件に従って送信し、各基地局側装置1000は、受信した認証用データに署名を行って認証装置1020に送信する。認証装置1020は、送信された署名を検証し、不正に切断された基地局側装置1000を検出した場合に、前記サービスIDに対応する鍵を更新した新しい鍵テーブル1030を各基地局側装置1000へ送信する。

【0115】図22は本実施形態の基地局の監視処理の処理手順を示すフローチャートである。図22に示す様にステップ2201で認証装置1020の監視データ送信処理部1313は、所定時間の経過等の条件が成立すると、ネットワークに接続された基地局側装置1000を監視する為の乱数等の認証用データと、監視用の認証用データであることを示すサービスIDとを格納したパケットをネットワーク上に送出する。

【0116】各基地局側装置1000の生存通知処理部1115は、ネットワーク上に送出されているパケットのサービスIDを調べ、監視用の認証用データが送出されている場合にはその認証用データを受信して、生存通知であることを示すサービスIDに対応した鍵を鍵テーブル1030から読み出して前記認証用データを暗号化し、その暗号化認証用データと、生存通知であることを示すサービスIDとを格納したパケットをネットワーク上に送出する。

【0117】ステップ2202で認証装置1020は、ネットワーク上に送出されているパケットのサービスIDを調べ、生存通知が送出されている場合にはその生存通知を受信してステップ2203へ進む。

【0118】ステップ2203で鍵更新処理部1314は、前記送信された生存通知中の暗号化認証用データをそのサービスIDに対応した鍵を用いて復号化する。ステップ2204では、前記送信した認証用データと前記復号化した認証用データが一致するかどうかを調べ、両者が一致する場合にはステップ2205へ進む。

【0119】ステップ2205では、ネットワーク上に接続された全ての基地局側装置1000からの生存通知を受信したかどうかを調べ、まだ生存通知を受信していない基地局側装置1000がある場合にはステップ2202へ戻る。

【0120】ステップ2202では、ネットワーク上に送出されているパケットのサービスIDを調べ、生存通

知が送出されていない場合にはステップ2206へ進む。ステップ2206では、認証用データを送出してから所定の時間が経過したかどうかを調べ、所定の時間が経過した場合には不正に切断された基地局側装置1000があるものとしてステップ2207へ進む。

【0121】ステップ2207で鍵更新処理部1314は、サービスIDに対応する鍵を更新した鍵テーブル1030を生成し、鍵更新であることを示すサービスIDに対応した鍵で前記更新後の鍵テーブル1030を暗号化して鍵配布データを生成し、その鍵配布データと、鍵配布であることを示すサービスIDとを格納したパケットをネットワーク上に送出する。

【0122】各基地局側装置1000は、ネットワーク上に送出されているパケットのサービスIDを調べ、鍵更新による鍵配布データが送出されている場合にはその鍵配布データを受信して、鍵更新であることを示すサービスIDに対応した鍵を鍵テーブル1030から読み出して前記鍵配布データを復号化し、その復号化した鍵データをROM1103中の鍵テーブル1030に格納して鍵データの更新を行う。

【0123】前記の様に本実施形態の通信セキュリティ保持システムでは、新規にネットワーク接続された基地局側装置1000が正規の基地局として認証された後に鍵テーブル1030の内容を配送し、また不正に切断された基地局側装置1000を検出して鍵テーブル1030の内容を変更するので、サービスIDに対応する鍵を用いた暗号化通信のセキュリティを高めることが可能である。

【0124】以上説明した様に本実施形態の通信セキュリティ保持システムによれば、送信データの内容を示すサービスIDに対応した鍵で送信データを暗号化してネットワーク上へ送出するので、送信先を特定しない放送型の通信を用いた場合でもその通信のセキュリティを高めることが可能である。

【0125】

【発明の効果】本発明によれば認証確立時に発行された認証継続用鍵によってそれ以後の認証継続時の認証を行うので、移動局鍵を用いた処理量を削減し、移動局と基地局との間の通信セキュリティを高めることが可能である。

【図面の簡単な説明】

【図1】実施形態1の通信セキュリティ保持システムの概略構成を示す図である。

【図2】実施形態1の基地局側装置1000の概略構成を示す図である。

【図3】実施形態1の移動局側装置110の概略構成を示す図である。

【図4】実施形態1の認証確立処理の概要を示す図である。

【図5】実施形態1の認証確立処理のシーケンスを示す

図である。

【図6】実施形態1の認証継続処理の概要を示す図である。

【図7】実施形態1の認証継続処理のシーケンスを示す図である。

【図8】実施形態1の基地局側装置100による移動局側装置110の認証確立処理及び認証継続処理の処理手順を示すフローチャートである。

【図9】実施形態1の移動局側装置110から基地局側装置100への認証確立要求処理及び認証継続要求処理の処理手順を示すフローチャートである。

【図10】実施形態2の通信セキュリティ保持システムの概略構成を示す図である。

【図11】実施形態2の基地局側装置1000の概略構成を示す図である。

【図12】実施形態2のゲートウェイ装置1010の概略構成を示す図である。

【図13】実施形態2の認証装置1020の概略構成を示す図である。

【図14】実施形態2の自律分散システムでの暗号通信処理の概要を示す図である。

【図15】実施形態2の基地局側装置1000からのデータ送信処理の処理手順を示すフローチャートである。

【図16】実施形態2の鍵テーブル1030の一例を示す図である。

【図17】実施形態2のゲートウェイ装置1010でのデータ受信処理の処理手順を示すフローチャートである。

【図18】実施形態2の新規基地局の認証処理の概要を示す図である。

【図19】実施形態2の新規基地局の認証要求処理の処理手順を示すフローチャートである。

【図20】実施形態2の認証装置1020による新規基地局の認証処理の処理手順を示すフローチャートである。

る。

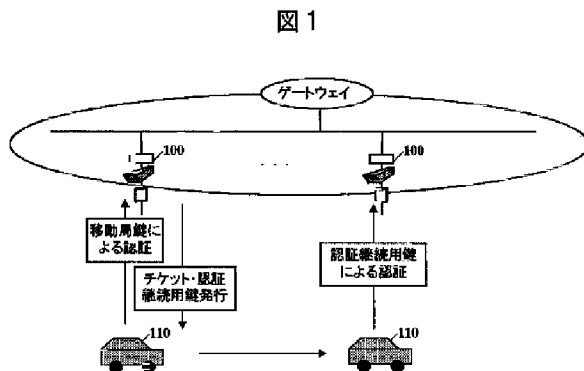
【図21】実施形態2の基地局の監視処理の概要を示す図である。

【図22】実施形態2の基地局の監視処理の処理手順を示すフローチャートである。

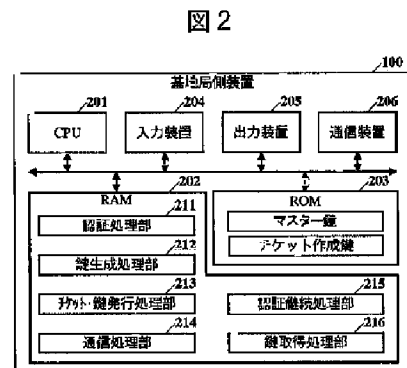
【符号の説明】

100…基地局側装置、110…移動局側装置、201…CPU、202…RAM、203…ROM、204…入力装置、205…出力装置、206…通信装置、211…認証処理部、212…鍵生成処理部、213…チケット・鍵発行処理部、214…通信処理部、215…認証継続処理部、216…鍵取得処理部、301…CPU、302…RAM、303…ROM、304…入力装置、305…出力装置、306…通信装置、311…認証要求処理部、312…チケット・鍵取得処理部、313…通信処理部、314…認証継続要求処理部、1000…基地局側装置、1010…ゲートウェイ装置、1020…認証装置、1030…鍵テーブル、1101…CPU、1102…RAM、1103…ROM、1104…入力装置、1105…出力装置、1106…通信装置、1111…暗号化処理部、1112…パケット送出処理部、1113…接続通知処理部、1114…署名送信処理部、1115…生存通知処理部、1201…CPU、1202…メモリ、1203…磁気ディスク装置、1204…入力装置、1205…出力装置、1206…CD-ROM装置、1207…通信装置、1211…復号化処理部、1212…データ処理部、1301…CPU、1302…メモリ、1303…磁気ディスク装置、1304…入力装置、1305…出力装置、1306…CD-ROM装置、1307…通信装置、1311…認証用データ送信処理部、1312…鍵送信処理部、1313…監視データ送信処理部、1314…鍵更新処理部。

【図1】

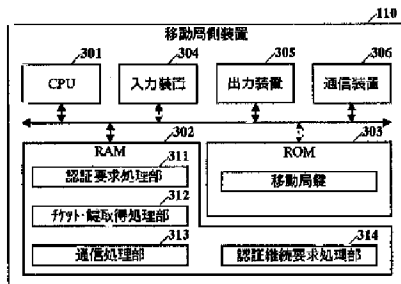


【図2】



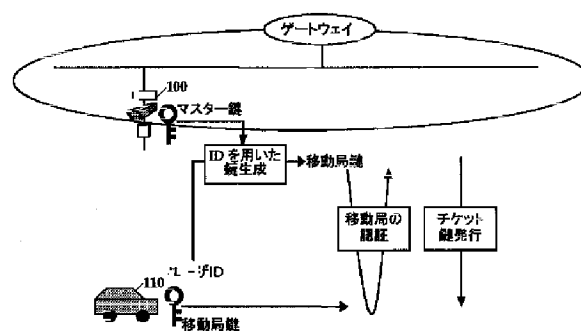
【図3】

図3



【図4】

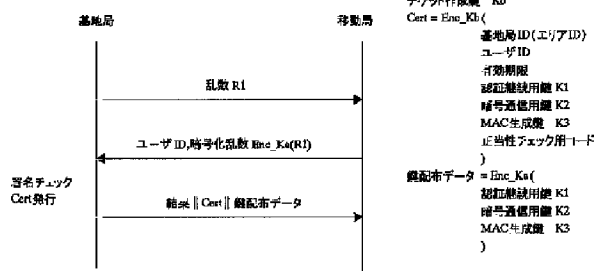
図4



【図5】

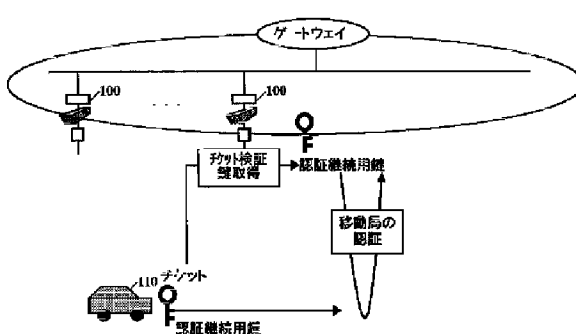
図5

認証確立時の処理



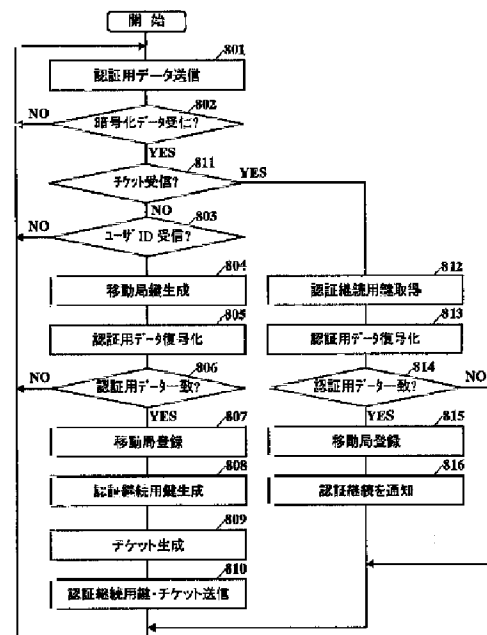
【図6】

図6



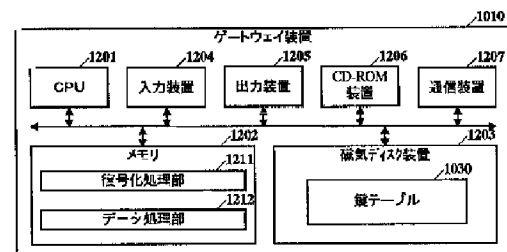
【図8】

図8

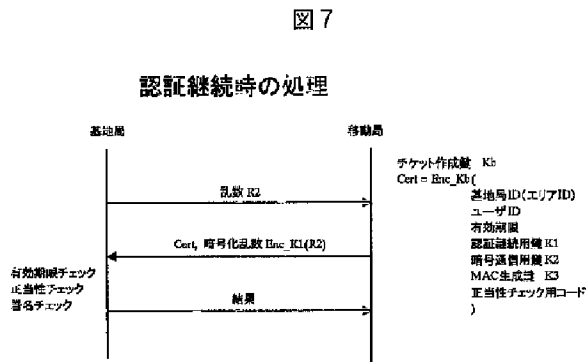


【図12】

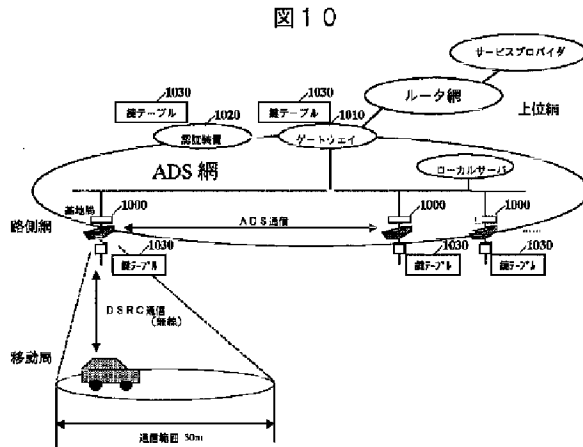
図12



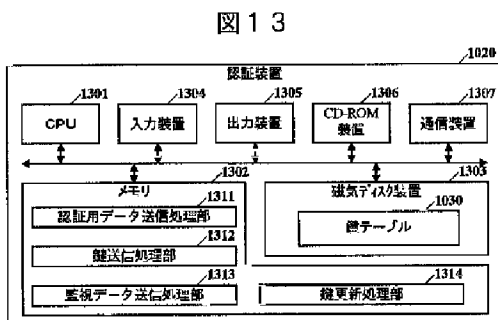
【図7】



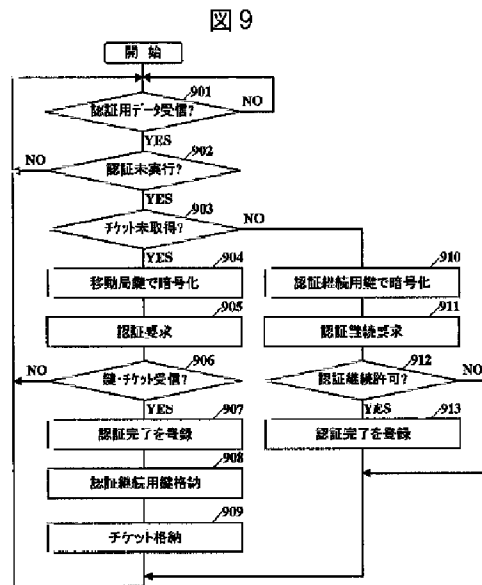
【図10】



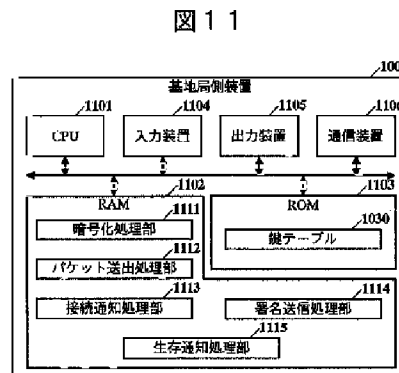
【図13】



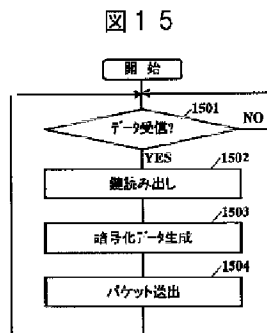
【図9】



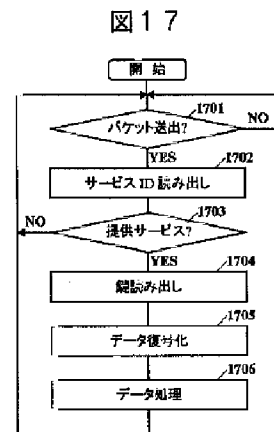
【図11】



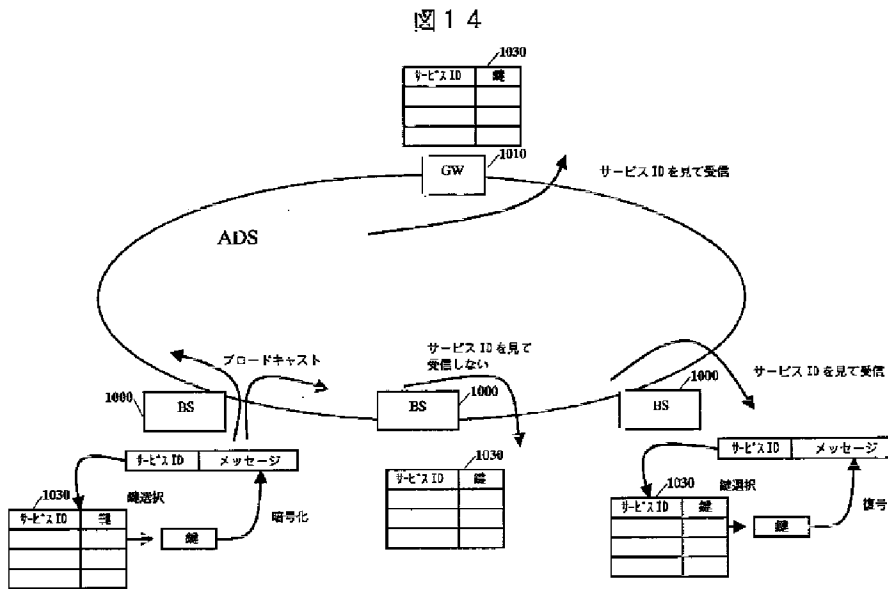
【図15】



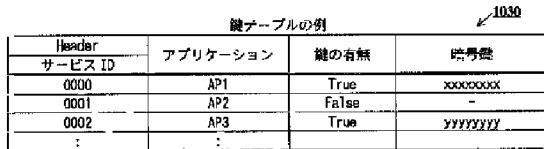
【図17】



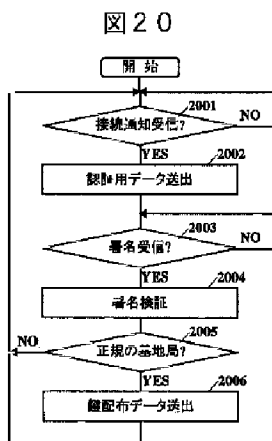
【例 14】



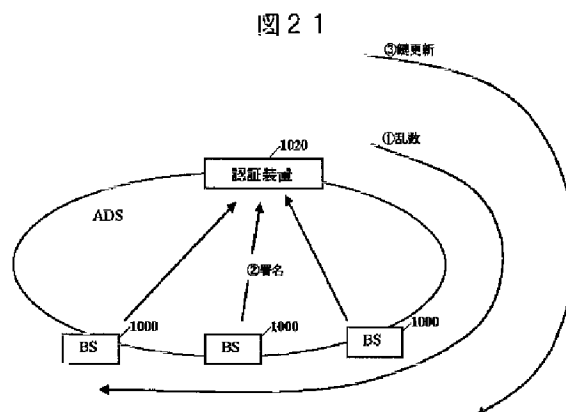
【例 16】



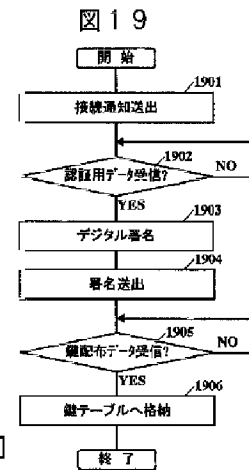
【図20】



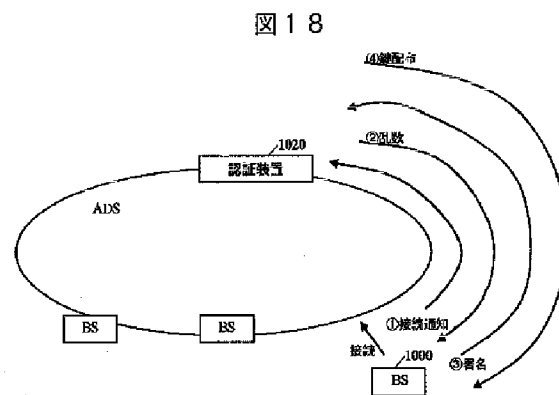
【图 2-1】



【例 19】

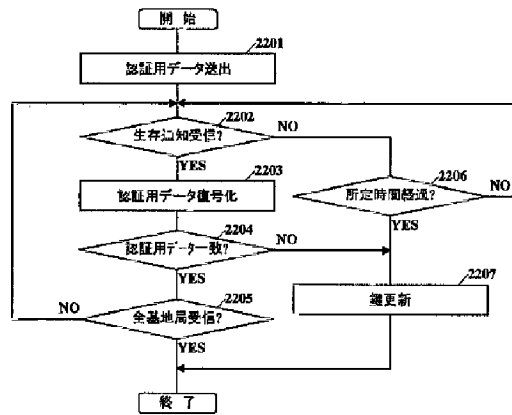


【例 18】



【図 22】

図 22



フロントページの続き

(72)発明者 瀬戸 洋一

神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

Fターム(参考) 5J104 AA07 AA09 AA16 EA04 EA17

EA26 GA05 KA02 KA04 LA06

NA02 PA01

5K067 AA33 BB03 BB04 BB21 BB43

CC08 DD17 EE00 EE02 EE10

HH21 HH22 HH24